Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

KENTUCKY CABINET
FOR HEALTH AND FAMILY SERVICES

010.102 Data/Media Security

Version 2.1
January 27, 2017

Revision History

Date	Version	Description	Author
11/16/2006	1.0	Effective Date	CHFS OATS Policy Charter Team
1/27/2017	2.1	Revision Date	CHFS OATS Policy Charter Team
1/27/2017	2.1	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	1/27/2017	ROBERT PUTT	

Table of Contents

1 010.102 Data/Media Security

Category: 010.000 Logical Security

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a data security policy. This document establishes the agency's Data/Media Security Policy to manage the reduction of risks, and provides guidelines for security best practices regarding data and media security.

1.2 Scope

The scope of this policy applies to all CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer, application, and data communication systems.

1.3 Roles and Responsibilities

1.3.1 OATS Information Security Team

Responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This team is responsible for the adherence of the CHFS Data/Media Security Policy.

1.3.2 Privacy Lead

The individual(s) responsible for providing security and privacy guidance for protection of Personally Identifiable Information (PII), Electronic Protected Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of the CHFS SDLC Policy in concert with the OATS Information Security (IS) Team.

1.3.3 *CHFS Staff and Contract Employees*

Individual(s) must adhere to the CHFS Data/Media Security Policy as well as referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system.

1.4 Management Commitment

This policy has been approved by OATS Division Directors and the OATS Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy.

1.5 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet for access to applications or systems. All organizational entities that interact with CHFS systems, within OATS, are subject to follow requirements outlined within this policy.

1.6 Compliance

CHFS abides by the security and privacy requirements established in the National Institute of Standards and Technology (NIST), the Internal Revenue Services (IRS), the Social Security Administration (SSA), the Centers for Medicare and Medicaid Services (CMS), as well as other federal and state organizations as the official guidance domain for this policy.

2 Policy Requirements

2.1 General

All data and media must be sufficiently protected and monitored, consistent with CHFS IT policies and procedures, to prevent unauthorized use, modification, disclosure, destruction, and denial of service. OATS IS Team and Enterprise documentation must apply security controls in a manner that is consistent with the value and classification of the data, as defined. Access to data/media is assigned on the “Principal of Least Privilege”, to users accessing only the information necessary to perform their job function(s). Access to data/media shall be subject to approval by appropriate management personnel. This policy shall align with all Commonwealth Office of Technology (COT) enterprise IT policies that pertain to data/media security.

2.2 Definitions

- Non-Electronic Media- Non-electronic media includes but is not limited to, hard copy or physical representation of information (ex. paper copies, printouts, drums, microfilm, handwritten notes, etc.).
- Electronic media includes but is not limited to, physical electronic media used to store information (ex. diskettes, magnetic tapes, desktops, laptops, hard drives, read only memory, compact disks, thumb drives, mobile devices, tablets, etc.). Laptops and mobile devices ~~should~~ will be configured by COT Desktop Support to ensure the maximum level of security necessary to protect any sensitive data downloaded to that drive.

2.3 Data Classification

All CHFS data will be reviewed by the owner of the data and reviewed by OATS Information Security (IS) Team to determine its level of sensitivity and/or criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls will be applied. Any exception to this policy requires approval by OATS IS Team (see section 4 Exceptions below).

2.4 External Markings

All sensitive data/media shall contain external restrictive markings for easy identification as CHFS property. The restrictive markings, including destruction and retention instructions are affixed to all media output to warn users of the degree of protection needed. Media belonging to external vendors, in the possession of CHFS employee/contractors, is subject to the same restrictive markings.

2.5 Reproduction

When sensitive cabinet and/or agency data/media is reproduced in total or in part, the reproductions shall bear the same restrictive markings as the original. Reproductions of sensitive data/media shall be kept to the minimum number of copies required. All CHFS employees and contractors are responsible to ensure that any sensitive information that is printed to a shared printer is picked up immediately and stored securely.

2.6 Storage and Security

2.6.1 Non-Electronic Media

All sensitive and confidential data/media entering or leaving offices, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. Storage areas and the facilities used for sensitive data/media shall be secured by locking all cabinets and drawers.

2.6.2 Electronic Media

All sensitive and confidential data/media entering or leaving offices, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. As defined by COT Enterprise IT: CIO-072 Identity and Access Management Policy and CIO-092 Media Protection Policy all data/media must be securely stored and protected.

At no time shall any personal removable storage devices, devices not issued by the commonwealth, be attached to state owned workstations with the purpose of storing and/or retrieving electronic data/media.

2.7 Disposal/Destruction

2.7.1 Non-Electronic Media

No sensitive information shall be disposed of by any publically accessible means. Sensitive information shall be afforded special handling regarding its disposal/destruction. This may include the use of shredders and/or special burn facilities including approved vendor services contracted by the Commonwealth.

2.7.2 Electronic Media

All sensitive information on electronic media shall be properly disposed of in accordance with COT Enterprise IT: CIO-092 Media Protection Policy.

2.8 Shipping and Manual Handling

CHFS data/media shall not be supplied to vendors, contractors or other external organizations without properly executed contracts, agreements, (i.e. MOU, BAA, MOA, etc.), and confidentiality agreements. Contracts and agreements shall specify conditions of use, security requirements, and return dates. When shipping sensitive information, receipt of delivery must be verified, unless otherwise action/receipt is required by law or statutory regulation.

2.9 Facsimile Transmission

When all sensitive information is sent by fax, the recipient must first be notified of the time it will be transmitted and also agree that an authorized person will be present at the destination machine. An exception will be made if the area surrounding the fax machine is physically restricted to authorized personnel only.

When sensitive data/media is faxed, the transmittal must include a CHFS cover sheet that contains a confidentiality statement as defined and approved by each agency's management. Sensitive CHFS data must not be faxed via non-trusted intermediaries like hotel staff, rented mailbox store staff, etc.

2.10 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

When sensitive data is sent via the Internet or other unsecured media transmission facility, the data must be sent securely via one of the Commonwealth's approved methods (i.e. encryption, SSL, etc.) in accordance with best practices as defined by COT Enterprise IT: CIO-091 Enterprise Information Security Program.

3 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

4 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS OATS IT Policy: 070.203.

5 Review Cycle

This policy is annually reviewed and revised on an as needed basis.

6 References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-072- Identity and Access Management Policy
- Enterprise IT Policy: CIO- 091- Enterprise Information Security Program Policy
- Enterprise IT Policy: CIO-092- Media Protection Policy
- Internal Revenue Services (IRS) Publication 1075
- KRS 434.855 - Misuse of computer information
- KRS 514.030 - Theft by unlawful taking or disposition
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Framework